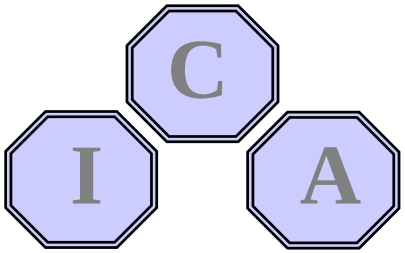
LAC
Little eArth Corporation

侵害事例に基づくケーススタディ

Case Study of Computer Security Incident

～Windows編～



株式会社ラック
倉林 俊介
shunsuke.kurahayasi@lac.co.jp
http://www.lac.co.jp/security/

本セッションの概要

LAC
Little eArth Corporation

- Windowsにおける典型的なインシデント事例を紹介
- 事例や公開情報に基づく最近の傾向を解説
- 効果的な対策につなげるための考え方を紹介

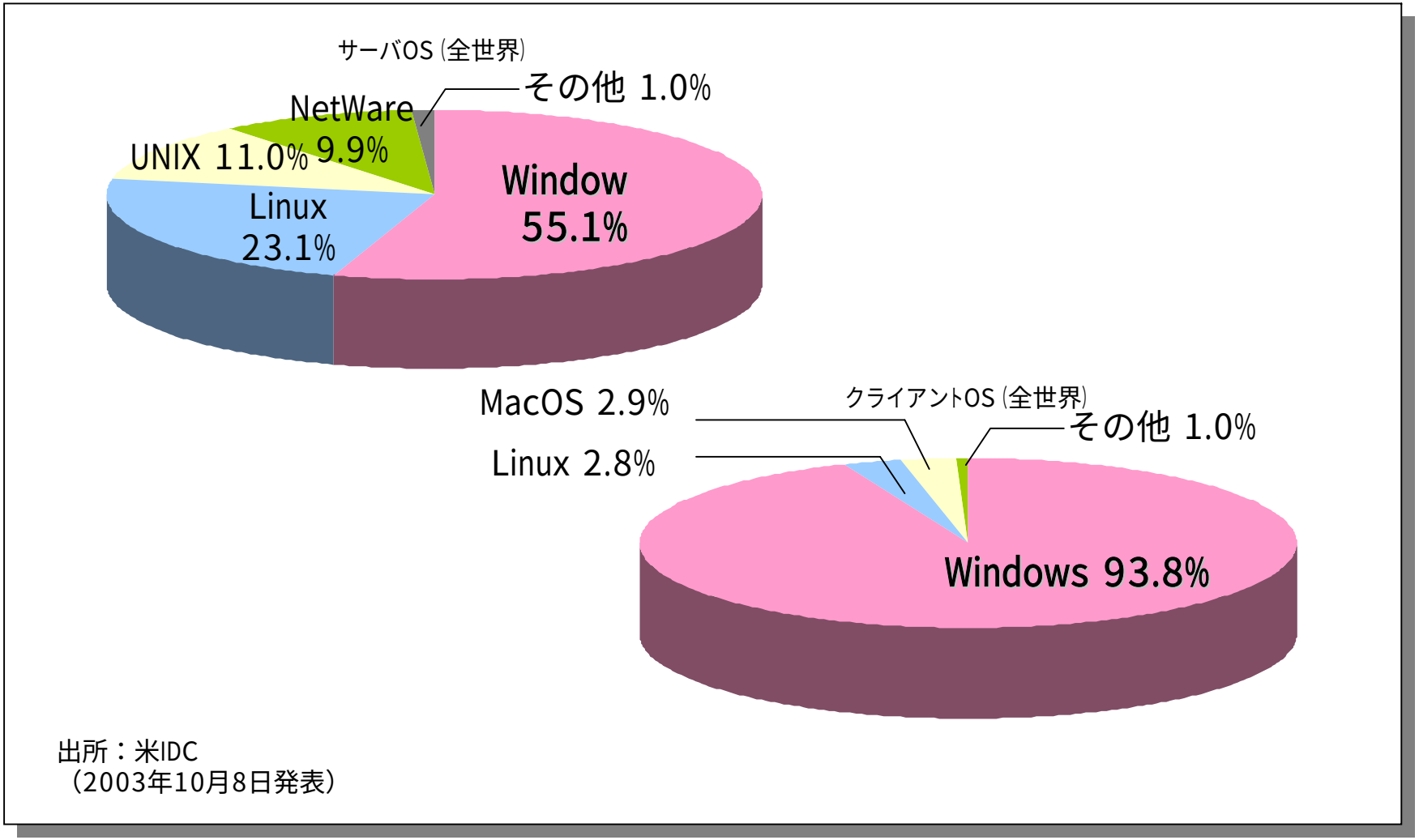
目次

- はじめに
- ＜ＣＡＳＥ１＞ 外部からの侵害
- ＜ＣＡＳＥ２＞ 内部からの侵害
- 最近のトレンド
- 効果的な対策のススメ

A little leak will sink a great ship.

はじめに

市場におけるWindowsのシェア



出所：米IDC
（2003年10月8日発表）

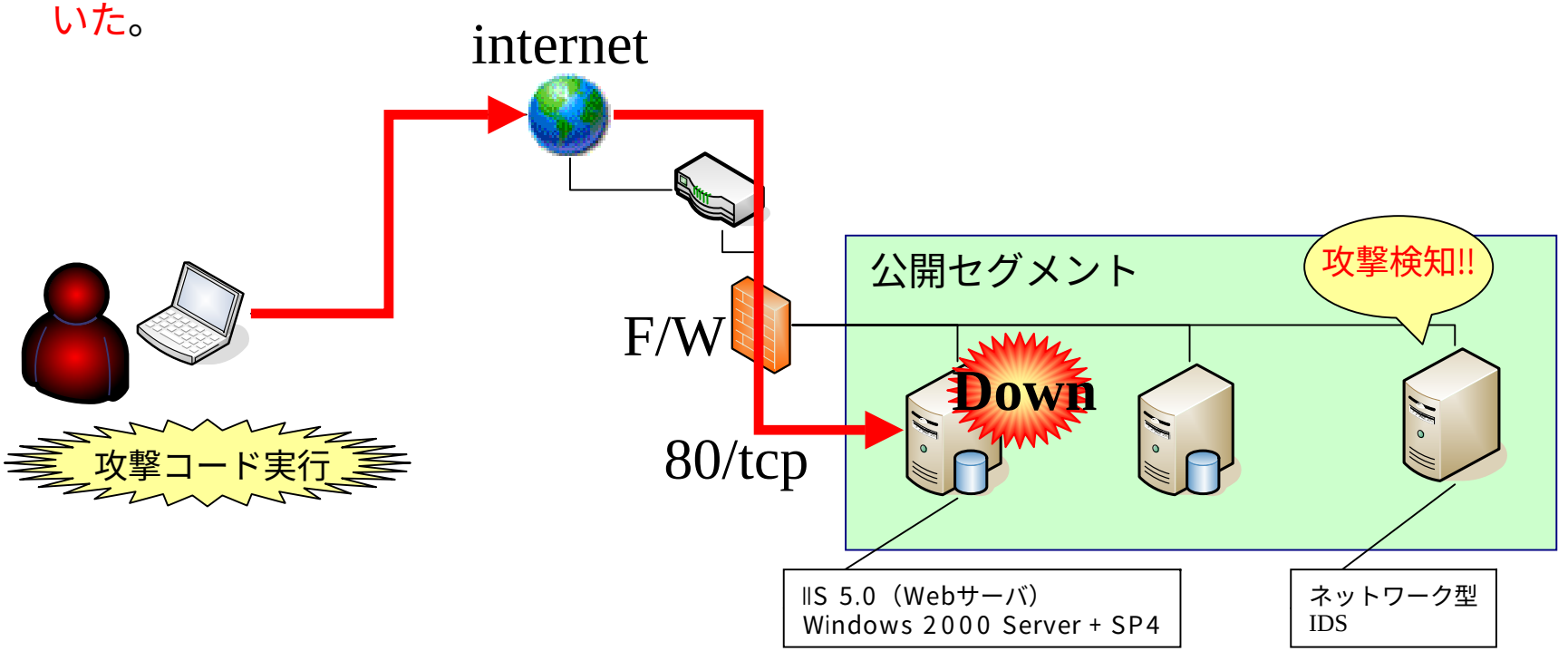
＜ＣＡＳＥ１＞ 外部からの侵害

サ　ー　ビ　ス　拒　否　攻　撃
Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ　Ａｔｔａｃｋ

<CASE１> 外部からの侵害

インシデント概要

２００４年１０月１３日深夜、社外に公開しているWebサーバが攻撃を受けて停止、同サーバ上で提供していた会員向けサービスが一時的に利用できなくなった。同サイトではF/Wに加え、万が一の不正アクセスに備えてネットワーク型IDSを導入していた。しかし、攻撃を受けたサーバでは自社開発のWebアプリケーションが稼働しており、アプリケーションの互換性を重視してパッチの適用を控えていた。



セキュリティホール概要

WebDAV XML Message ハンドラの脆弱性によりサービス拒否が起こる (824151) (MS04-030)

Microsoft XML Parser に起因する問題。意図的に作成したWebDAVリクエストをHTTP経由でターゲットに繰り返し送信することで、対象をサービス拒否状態に陥れることが可能となる。

対象システム

- Microsoft Internet Information Services 5.0
- Microsoft Internet Information Services 5.1
- Microsoft Internet Information Services 6.0
- Microsoft Windows 2000 Advanced Server SP4 以前
- Microsoft Windows 2000 Datacenter Server SP4 以前
- Microsoft Windows 2000 Server SP4 以前
- Microsoft Windows 2000 Professional SP4 以前
- Microsoft Windows XP Professional SP1 以前
- Microsoft Windows Server 2003 Standard Edition
- Microsoft Windows Server 2003 Enterprise Edition
- Microsoft Windows Server 2003 Datacenter Edition
- Microsoft Windows Server 2003 Web Edition

対策方法

１．セキュリティ修正プログラムの適用
２．WebDAVの無効化

参照元:
http://www.microsoft.com/japan/technet/security/bulletin/MS04-030.asp

インシデント対応

公開セグメントに設置していたIDS（侵入検知システム）が攻撃を検知し、警報を発信。深夜であったためサーバ管理者の対応が遅れ、サーバの停止時間は3時間に及んだ。対応完了後に原因を調査し、Webサイトにサービス停止に関する謝罪文（下図）を掲載したところ、今度は顧客から個人情報の安否に関する問い合わせが殺到した。

サービス利用停止のお詫び

2004年10月22日

2004年10月13日深夜ごろ、当サイトが外部からの不正アクセスを受け、アクセス不能になるという事態が発生いたしました。お客様には大変ご迷惑をおかけいたしましたことをお詫びいたします。なお、当社では全力を挙げて原因の解明、及び再発防止に取り組み、お客様が寄り安心してご利用いただけるサービス作りを目指してゆく所存でございます。今後ともよろしくお願いいたします。

株式会社○○
代表取締役　△△■■

事例における問題点

➢不要な機能（WebDAV）が有効化されていた

- ✓ 構築時にセキュリティが意識されない（デフォルトのまま使用？）
- ✓ 必要な機能とそうでないものの選定が行えていない

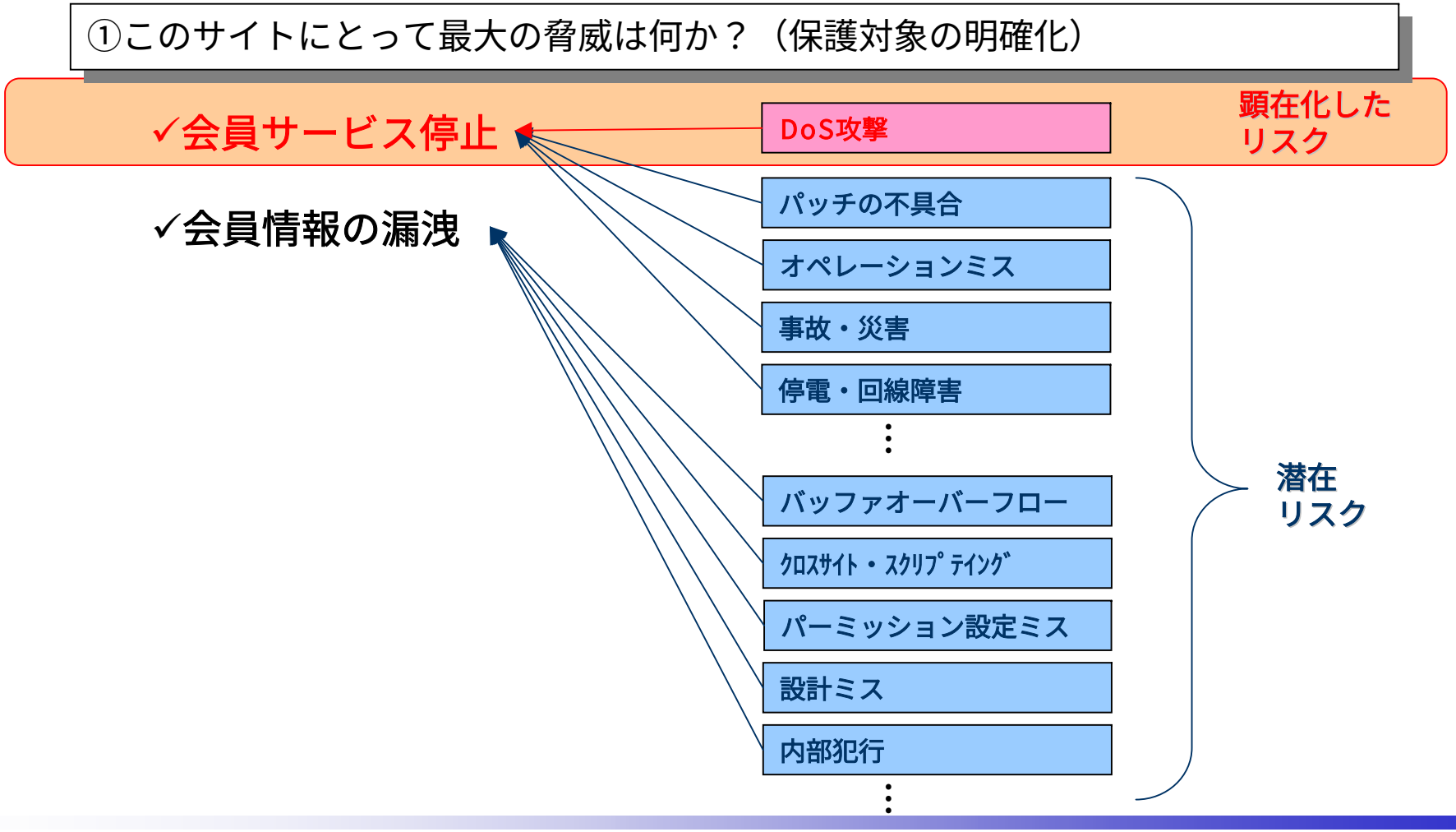
➢パッチが適用できなかった

- ✓ そもそも、セキュリティホールの存在が認識されていない
- ✓ アプリケーションとの互換性の問題
- ✓ 運用委託のケースではパッチ適用までにタイムラグが生じるケースも

➢ファイアウォールやIDSを過信（誤解？）していた

- ✓ 許可されているサービスを利用した攻撃は防げない
- ✓ 攻撃を検知できても止めることはできない

改善のための考察



改善のための考察

②セキュリティホールを塞げないのであれば、**問題の切り分けや代替策の検討を行うべき**

✓パッチの適用による不具合を極力避けたい場合に、セキュリティホールが悪用される可能性を最小限に抑えるためには何が出来るか？
（ex. サーバの機能の最小化、冗長化、危険度も含めたセキュリティ情報収集、テスト環境の準備 等）
✓ファイアウォールで防げないのはどんな攻撃？
（ex. Port80を経由したDoS、バッファオーバーフロー、XSS 等）
✓IDSで攻撃を検知してからアラート発信までのタイムラグは？
✓アラートをキャッチしてから対応までにどのくらい時間が掛かる？
（ex. 昼の場合/夜の場合）
✓既存の対策を組み合わせてできることはないか？
（ex. IDSとF/Wの連携 等）
✓問題が起こってしまった場合の対応について、事前に準備できることはないか？
（ex. 不測事態対応マニュアルの作成、従業員・関係機関の緊急連絡先の特定、謝罪文の雛形準備 等）

等々・・・

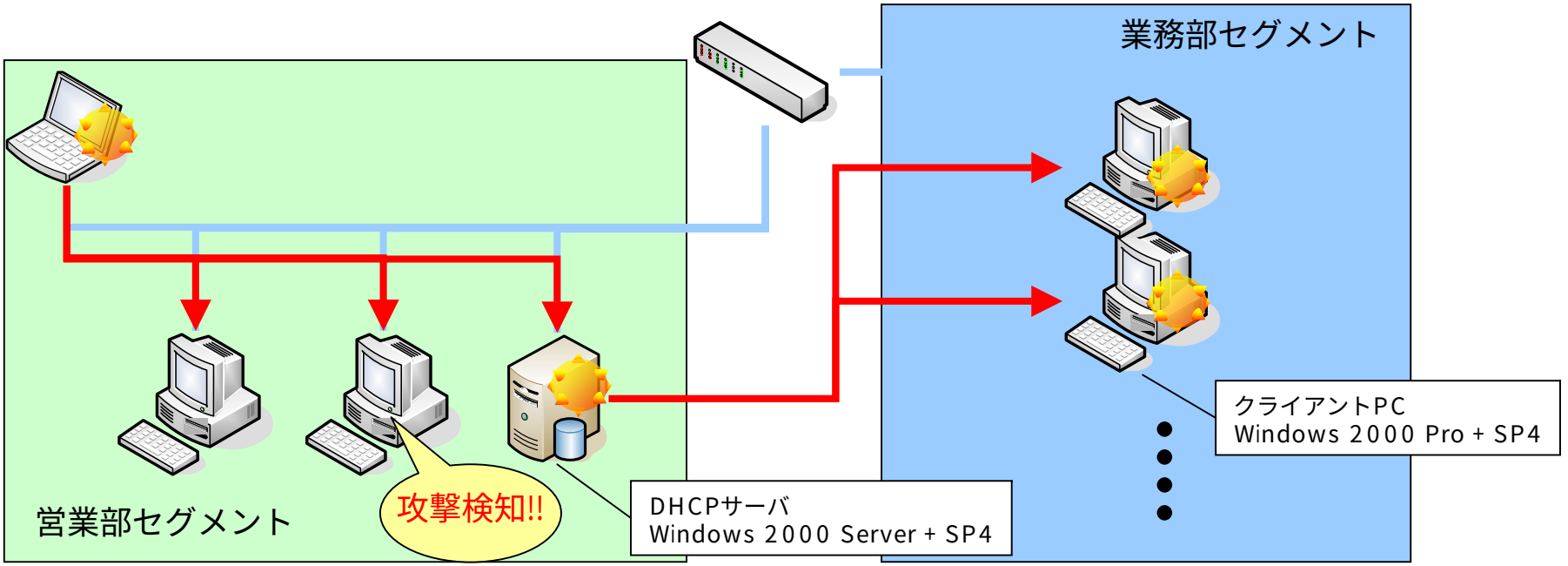
＜CASE2＞ 内部からの侵害

ウィルス・ワーム感染
The infection of Computer Virus / Worm

<CASE2> 内部からの侵害

インシデント概要

2003年8月11日早朝、社外に常駐していた社員が社内ミーティングのため、ノートPCを営業部セグメントに接続。このマシンはBlasterワームに感染しており、営業部のDHCPサーバが感染したほか、別セグメントでOSの再インストールを行っていた社員のPC等に感染が拡大した。この企業では以前から情報セキュリティポリシーを策定する等、セキュリティ向上のための積極的な取り組みを行っていた。



ワーム概要

MS Blast（Blaster または Lovsan ワーム）

Microsoft 社製の主要なOSに発見されたRPC DCOMインターフェースの脆弱性（MS03-026）を悪用して感染拡大し、バックドア作成、 Microsoft 社のWebサイト「Windows Update」に対してのDoS攻撃等を行うワーム。脆弱性のPOCコードが公開された１ヵ月後に出現、大きな被害をもたらした。

対象システム

-Microsoft Windows NT 4.0（SP6a以前の全バージョン）
- Microsoft Windows 2000 （SP4以前の全バージョン）
- Microsoft Windows XP（SP1以前の全バージョン）
- Microsoft Windows Server 2003

参照元:
http://www.microsoft.com/japan/technet/security/bulletin/ms03-026.asp

対策方法

予防策

１．セキュリティ修正プログラムの適用
２．DCOMの無効化
３．ファイアウォールによるフィルタリング
（※Windows XP、Windows Server 2003のみ）

感染後の対処

１．ネットワークからの隔離
２．駆除ツールの実行
３．セキュリティ修正プログラムの適用

インシデント対応

ポリシーどおりパーソナルファイアウォールを導入していた他の社員が感染マシンからの攻撃を検知、情報システム部に通報。直ちに感染マシンの切り離しを実施したため、大事には至らなかった。この事件を受けて情報システム部では、社内イントラに以下のような通知文を掲載し、注意喚起を行った。

ウィルス感染への注意喚起

2003年8月25日

今月11日の早朝、社内ネットワークで悪質なコンピュータウィルスの感染が発見されました。社員各位はセキュリティポリシーを再度確認のうえ、下記の対処を必ず実施していただきますようお願いいたします。

1．定期的なWindows Updateの実施
2．ウィルス対策ソフトの常駐設定
3．パーソナルファイアウォールソフトによる監視設定

本件に関するお問い合わせはこちらまで
情報システム部 ××
E-mail XX@sample.co.jp
内線 YYYY

事例における問題点

➢情報セキュリティポリシーの遵守

✓ 情報セキュリティポリシーが徹底されていなかった
（パッチの適用、ウィルス定義ファイルの更新）

➢情報セキュリティポリシーそのものの不備

✓ ポリシーだけでは内容があいまいでどうすればよいか分からない
✓ 最新のパッチを適用するためにはネットワークにつなぐ必要がある
✓ セキュリティ設定の実施は利用者任せだった

➢内部ネットワークは制限が少ない

✓ 外側にはファイアウォールがあるが、内部はスカスカ
※Blasterワームへの感染事例はほとんどが外部からの持込によるものだった

改善のための考察

①情報セキュリティポリシーをどうやって遵守させるか？

情報セキュリティポリシー

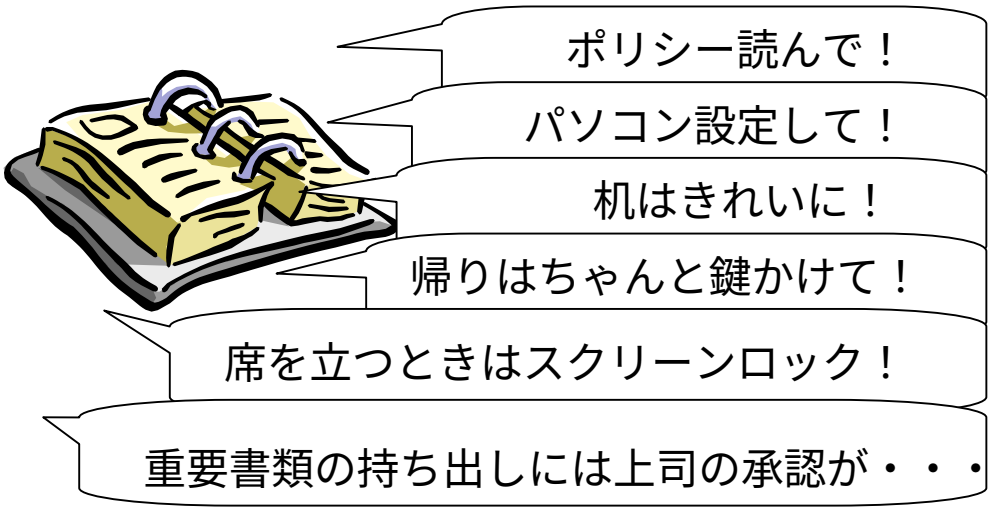
第XX条（クライアントコンピュータ利用時の対策）

・クライアントコンピュータのOS、ソフトウェアは、常に最新の状態に維持すること
・クライアントコンピュータには、ウィルス対策ソフトウェアを導入すること
・ウィルス対策ソフトウェアのウィルス定義ファイルは、常に最新の状態に維持すること
・クライアントコンピュータでは、定期的にウィルス検査を実施すること
・クライアントコンピュータでは、受信した電子メールのウィルス検査を実施すること
・インターネットからファイルのダウンロードを行った際には、ファイルを開く前に必ずウィルス検査を実施すること
・クライアントコンピュータには、業務上必要でないソフトウェアを導入しないこと

改善のための考察

➢情報セキュリティポリシーを遵守させるために克服すべき障害は何か？

✓一般利用者はセキュリティ（コンピュータ？）に詳しくない。
（※管理職は、もっと詳しくない。）
✓情報システム部は、説明が下手・・・（-_-;）。
✓みんな業務が忙しい（面倒なことはやってくれない。）



改善のための考察

➢ある程度自動化して、利用者の負担を減らす努力は必要。

例えば・・・

◆情報システム部ががんばる（※一元管理）

クライアントPCは情報システム部があらかじめ必要な設定を行った上で利用させる

- ✓購入機器の選定
- ✓起動・ログインパスワード設定
- ✓Windows の自動更新設定（更新には社内サーバを使用）
- ✓ウィルス対策ソフトのリアルタイム検知設定
- ✓ウィルス定義ファイルの自動更新設定
- ✓管理者権限の剥奪（設定変更をさせない）
- ✓セキュリティテンプレートの活用
- ✓Active Directory等による一元管理が理想的だが・・・

◆強制排除

ポリシー違反のPCはネットワークに接続させない

- ✓検疫ネットワーク等を活用

改善のための考察

➢利用者自身に「違反」を気づかせる（地道な）工夫を惜しまない。

◆警告の発信

気づかずに違反行為を行っている利用者に対し、警告を発することで違反に気づかせる。

- ✓ＰＣの無断持込を上司が注意
- ✓無許可でネットワークに接続されたサーバを自動検出、一定時間後に切り離し
- ✓施錠されていない不在者の机、ロッカーへの張り紙
- ✓ネットワーク接続時にパッチ未適用であることを警告（検疫NW）

◆数値化

定期点検、巡回点検を実施して実施状況を数値化。

- ✓チェックリストの項目について実施率を部門別に数値化
- ✓実施率を競わせるのも効果的（※インセンティブが必要）
- ✓実施率が低い部門を放置せず、積極的に相談に乗る
（※ルールで縛り付けたり、非難しても実施率は向上しない）

改善のための考察

➢利用者のリテラシーを高める教育も重要。

◆全社一律の教育

情報セキュリティにおける「リスク」を分かりやすく解説し、ポリシーを守ることの重要性を理解してもらう。

- ✓e-Learningツール（LMS）の活用
- ✓理解度確認テストを実施し、成績優秀者へのインセンティブを用意するのも効果的。
- ✓教育は継続的に行うことが必要。
- ✓専門用語は厳禁。なるべく平易な言葉で説明すること。

◆階層別の教育

特に現場を束ねる管理職に対しては、それぞれの役割に加えて、部下を指導育成してもらうための情報を与えることが重要。

- ✓実施すべき内容をチェックリスト化

改善のための考察

➢情報セキュリティポリシーは定期的に見直す。

- ✓見直しを行わなければ、必ず形骸化する（技術の進歩は早い）
- ✓利用者からのフィードバックを汲み取り、適宜反映する（現実的に守れない条項はいつまでたっても守られない：当たり前ですが ^_^;）。
- ✓世間の動向や最新の技術についてアンテナを張りめぐらしておく。
- ✓継続的改善のためには、達成目標を明確にすることが重要（数値化等。例えばウィルス感染率 0.1%以下、教育実施率１００% 等）。

最近のトレンド

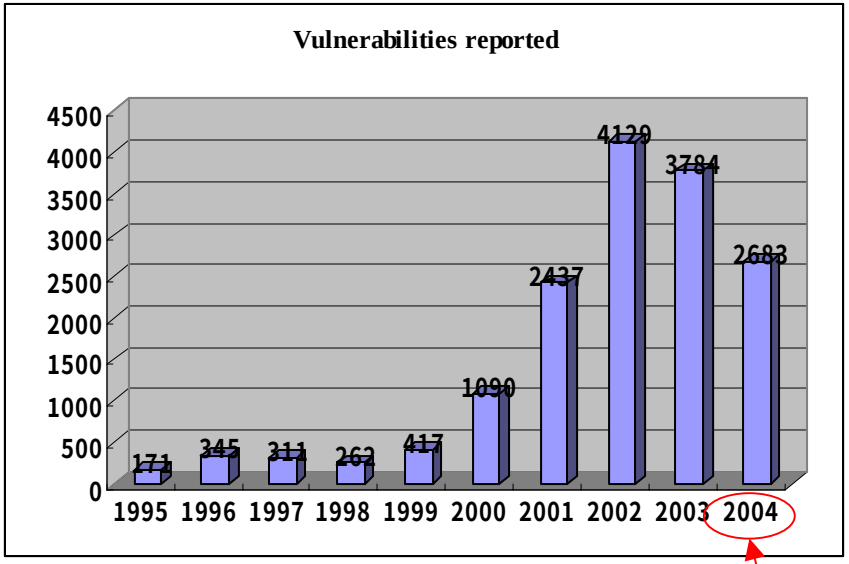
最近のトレンド

- セキュリティホールのマネジメント
- 個人情報保護法への対応

セキュリティホールのマネジメント

➢セキュリティホールの脅威は「予測不可能なもの」から「（ある程度）マネジメント可能」なものになりつつある

✓ ベンダーの積極的な取り組みにより、セキュリティホールの発見・報告数は増加傾向にある。



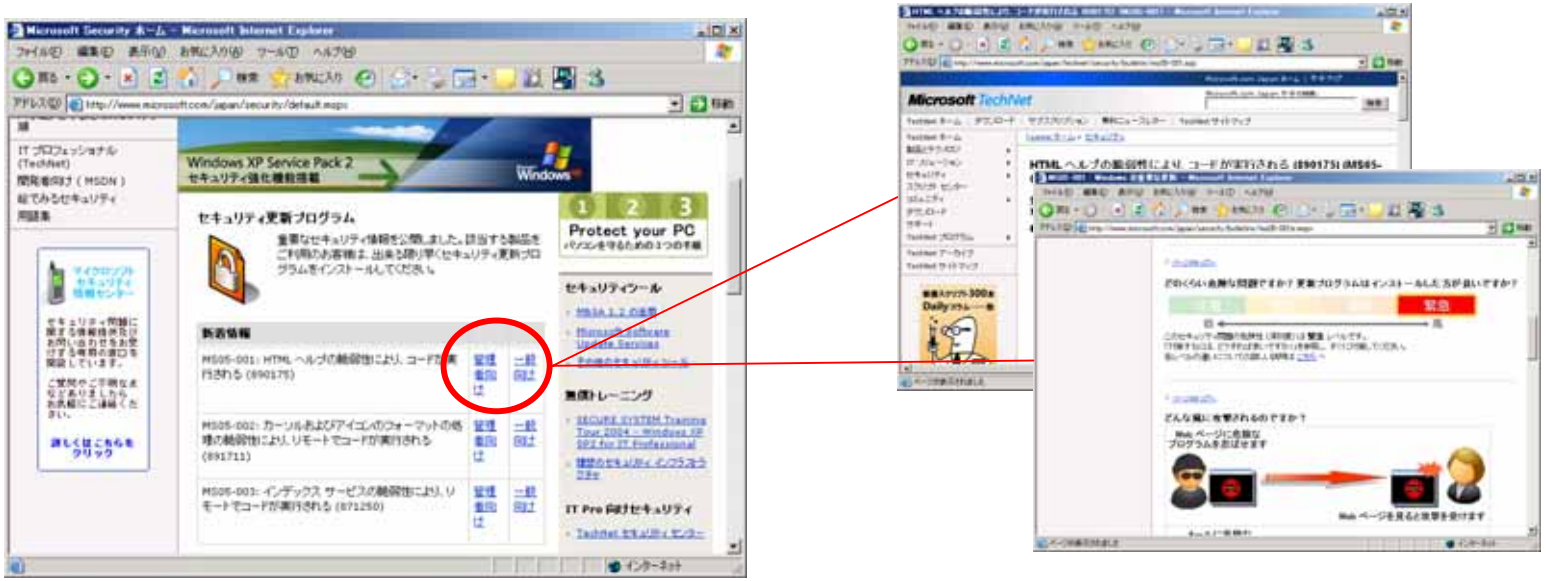
出典：CERT/CC Statistics 1988-2004
http://www.cert.org/stats/

※1Q～3Q

セキュリティホールのマネジメント

- セキュリティホールの脅威は「予測不可能なもの」から「（ある程度）マネジメント可能」なものになりつつある

  - ✓ 以前に比べてセキュリティ情報の内容が充実してきた（ex. 一般利用者向け/管理者向け/経営層向けの情報提供 等）。



セキュリティホールのマネジメント

- セキュリティホールの脅威は「予測不可能なもの」から「（ある程度）マネジメント可能」なものになりつつある

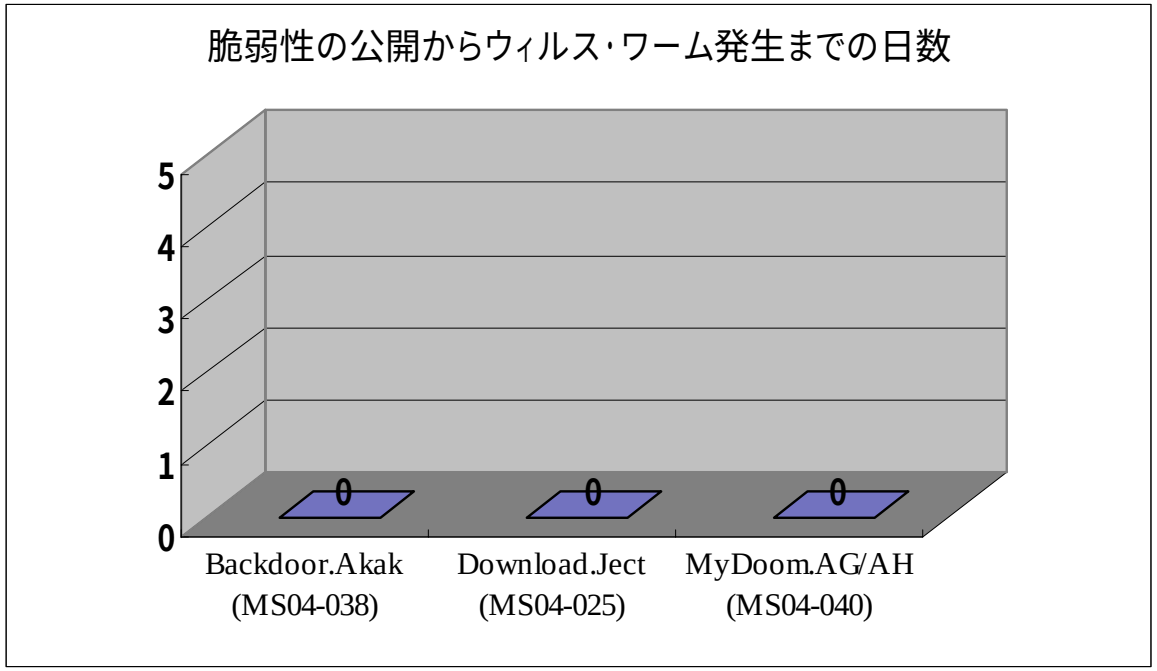
✓ セキュリティ製品の充実、多機能化により、典型的な攻撃の大部分は未然に対処することができるようになってきた。

ファイアウォール	単にアクセス制御だけでなく、簡易的なパケット検査機能を標準的に備える製品が増加。
侵入検知/防止システム	侵入防止（IDP/IPS）というコンセプトの製品。攻撃に対するより現実的なアクションが可能になった。
Webｱﾌﾟﾘｹｰｼｮﾝ防御ﾂｰﾙ	Webアプリケーションのセキュリティ強化に特化したアプリケーションファイアウォールが登場。
ウィルスゲートウェイ	ネットワークにおけるウィルス対策として、導入が進んでいる。
検疫ネットワーク	脆弱なコンピュータのネットワーク接続を強制的に排除できる。

セキュリティホールのマネジメント

- セキュリティホールの脅威は「予測不可能なもの」から「（ある程度）マネジメント可能」なものになりつつある

✓ 一方で、セキュリティホールの発見から攻撃手法のリリースまでの期間は限りなくゼロに近づいている（0-day Attackの脅威が増大）。



セキュリティホールのマネジメント

- セキュリティホールの脅威は「予測不可能なもの」から「（ある程度）マネジメント可能」なものになりつつある

✓ 汎用性の高いExploitが公開された場合には、無差別攻撃型のウィルスやワーム（しかも多機能！）が作成される危険が高まる。（特にWindowsでは顕著）

rank	name	type	related vulnerabilities
1	NETSKY	worm	○(MS01-020)
2	AGENT	trojan	
3	JAVA_BYTEVER	other	○(MS03-011)
4	AGOBOT	worm	○(MS03-026,MS03-001,MS03-007)
5	ISTBAR	trojan	
6	SDBOT	worm	○(MS03-026,MS03-001,MS03-007)
7	MYDOOM	worm	○(MS04-040)
8	RBOT	worm	○(MS03-026,MS03-007)
9	REDLOF	VB Script	○(MS00-075)
10	NACHI	worm	○(MS03-026)

参照元：トレンドマイクロ社 「ウイルス感染被害年間レポート　２００４年度」
http://www.trendmicro.com/jp/security/report/report/archive/2004/mvr2004-12.htm

個人情報保護法対応

- 個人情報保護法の完全施行が間近（4月）に迫り、各社が対応に本腰を入れ始めている

✓ 対応の指標として関係省庁からガイドライン提示されている。

経済産業省	個人情報の保護に関する法律についての経済産業分野を対象としたガイドライン
総務省	電気通信事業における個人情報保護に関するガイドライン
金融庁	金融分野における個人情報保護に関するガイドライン（※パブリックコメントの検討中？）

参考情報：個人情報の保護に係る関係省庁の検討状況
内閣府 国民生活政策ホームページ
http://www5.cao.go.jp/seikatsu/kojin/index.html

個人情報保護法対応

➢個人情報保護法の完全施行が間近（4月）に迫り、各社が対応に本腰を入れ始めている

✓ 内部犯行を防止する難しさが表面化しつつある。（ex. マスターキーを持つ支配人の犯行は防げない？）

◆システム上の管理者権限を持つ人物なら、どんな操作も思いのまま
→ログ改ざん
→重要情報へのアクセス、持ち出し
→盗聴
→監視システム停止

◆管理者権限を持つ人物による不正行為をどうやって防ぐか？
→運用でカバーする？（ex. 必ず二人一組のローテーションを構成）
→権限を分散させる？（ex. セキュアOSの利用）
→書き換え不可能なストレージを利用？

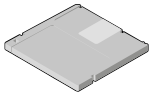
個人情報保護法対応

➢個人情報保護法の完全施行が間近（4月）に迫り、各社が対応に本腰を入れ始めている

✓ 大容量リムーバブルメディア等も新たな脅威として認知されつつある。

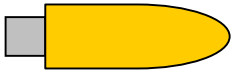
◆小型で且つ大容量のメディアが多数登場し、情報の持ち出しが容易に。
暗号化ツールやUSBポートの利用を制限するツール等も登場している。
→重要情報の持ち出し、転売（漏洩）のリスクが増大
→重要情報を保存したメディアの紛失、盗難のリスクが増大
→従業員のモラル・リテラシーに依存してしまう問題…

小型化・大容量化が進むリムーバブルメディア



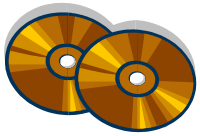
FD/MO

1MB～1.3GB



USBメモリ

8MB～2GB



CD/DVD/-R/RW

200MB～8.5GB

効果的な対策のススメ

効果的な対策のススメ

LAC
Little eArth Corporation

➢やっぱり「ＰＤＣＡ」が大切

Plan	：計画立案（リスク分析→対策計画）
Do	：計画に基づく対策の実施
Check	：対策の実施確認・効果測定（ウィルス感染発生率の推移 等）
Action	：対策内容の見直し、次期計画の立案

<P>計画の立案、人・モノ・金の確保 ・どこに、どんなリスクが、どれくらいある？ ・対策にかけられる予算は？ ・対策のために動ける要員は？ ・前回の反省点の反映	**<A>見直しの実施** ・予算・要員は十分だったか？ ・事件、事故が発生した原因は何だったのか？ ・問題が起こらないようにするためにはどうする？ ・世の中の動向は？
<D>「合理的な」対策 ・組織的対策 ・物理的対策 ・技術的対策 ・人的対策	**<C>実施状況を常にチェック** ・ポリシーを理解しているか？ ・ポリシーの内容が実践されているか？ ・事件、事故がどこで、どれくらい発生しているか？ ・事件、事故への対応は的確に行われているか？

➢これからのキーワード

➢「試行錯誤」の時代から、実績・ナレッジ「**活用**」の時代へ

✓自社に合った情報セキュリティマネジメントの確立を目指そう

➢「**自動化**」（情報収集から対策、実施確認まで）

✓自動アップデート、検疫ネットワーク等

➢対外的な「**アピール**」

✓セキュリティ投資にプラス効果を期待するなら戦略的にアピールしよう

➢「**内部統制**」の仕組み構築

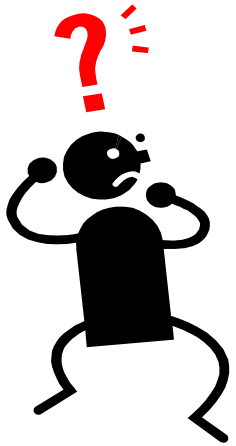
✓問題発生を未然に防ぐ組織作り

➢「**危機管理（Risk Management）体制**」の構築

✓情報セキュリティの枠を超えて、万が一への備えを万全に

質　問　タ　イ　ム

A n y　Q u e s t i o n s ?



ご清聴ありがとうございました